Avon and Somerset Police
SERVE. PROTECT. RESPECT.

Multi-Agency Overarching Information Sharing Agreement Tier 1

A standard overarching Information Sharing Agreement which can be used by all agencies within Avon and Somerset Constabulary policing area for sharing personal data.

If printed, copied or otherwise transferred from its originating electronic file this document must be considered to be an uncontrolled copy.
Amendments may occur at any time and you should always consult the principle electronic file or contact the Agreement owner for the latest version.

Contents

Version Control			
Edit	**Author**	**Version**	**Date**
Draft version raised at Chief Executives meeting (A&S Police HQ) for consultation	Jeff Hines	0.1	10.12.12
Final draft version	Jeff Hines	1.0	09.05.13
Minor revisions.	Jeff Hines	1.1	17.06.13
Agreement authorised by Acting Assistant Chief Constable Hayler, Avon an d Somerset Constabulary	Jeff Hines	1.2	17.06.13
Agreement reviewed. Meeting held at Police HQ with interested parties. Indemnity removed and minor format changes made.	Jeff Hines	1.3	26.06.14
Revised Agreement published	Jeff Hines	2.0	02.09.14
Bristol City Council Log added	Jeff Hines	2.1	19.09.14
South Glos. Council logo added	Jeff Hines	2.2	15.08.15
Original Protective Markings removed – document is OFFICIAL.- no markings required Document Reviewed Appendix B examples of signatory and date changed to Andy Marsh and March 2017	Jeff Hines	2.3	21.03.17
Revisions to reflect the changes to data protection legislation – GDPR and Data Protection Act 2018	Ellena Talbot	3	12.07.18
Minor changes of the author/owner of the document and reviewing schedule,	Kate Britton	3.1	05.02.19
Change GDPR > UK GDPR, email address	Kate Britton	3.2	24.06.21
Revised to reflect NPCC template	Michelle Radcliffe	3.3	09.02.22

Section 1 Information Sharing Agreement Tier 1 Information

Agreement Information	Reviewed by: (Name, Area/Dept.)	Date:
Signed off by Head of Department/Area:	Kate Britton, Data Protection Officer	February 2019
Reviewed for Code of Ethics Compliance:	Kate Britton, Data Protection Officer	February 2019
Start date:	June 2013	
Last reviewed:	February 2022	
Next due for review:	February 2023	

Section 2 About this Document

Avon and Somerset Constabulary operate a two-tier approach to information sharing. This over-arching agreement (Tier 1) is hosted by Avon and Somerset Constabulary and came in to effect on 17th June 2013. This has subsequently been reviewed and amended in accordance with UK GDPR/The Data Protection Act 2018.

This Information Sharing Agreement (ISA) Tier 1 provides a standard overarching agreement which can be used by all agencies within the Avon and Somerset Constabulary policing area for sharing personal data. This sets the guiding principles, ethos and standards for data sharing common to all agencies and is signed off once by the respective chief executive or equivalent.

An ISA Tier 2 can be used for all data sharing, ad hoc or regular, and it should be signed off by local managers; asset owners; asset assistant; asset guardians or custodians, anybody who consider themselves accountable for the data and the data exchange.

Contact or queries in relation to this agreement should be directed to:
The Data Protection Officer
Legal Services
Avon and Somerset Constabulary Police HQ
Valley Road
PO Box 37
Portishead
Bristol
BS20 8QJ
E-mail: *InformationSharing@avonandsomerset.police.uk*

Information Sharing Template Agreement (Tier 1)

Replace this text with name of partner

Replace this text with date of ISA

Administration:

The details of the organisation signed to this ISA (Tier 1)

Organisation	Address	ICO Registration Number

Introduction:

The significant benefits to service users, the wider public and to the legitimate activities of our organisations, derived from sharing timely, relevant and accurate data, both personal and other, have now long since been established. The widely recognised value and success of data sharing has however generated a plethora of agreements being developed between various partner agencies.

Although it is not a direct legal requirement, it is good practice to have an Information Sharing Agreements (ISA) in place where there is regular or semi-regular sharing of data, particularly personal data. Where disclosures are 'one off' in nature or do not involve personal data, there is no requirement for an ISA. For the purposes of this document the terms Information Sharing Protocol (ISP), Information Sharing Agreement (ISA) and Data Sharing Agreement (DSA) are interchangeable and have the same meaning.

Whilst this document prescribes the minimum acceptable standards at key stages of the sharing process, it will always be the responsibility of each partner to ensure that they comply with any legislation, national standards and local policy(s) applicable to them or to the processes in which they are engaged.

By setting the minimum standards and expectations for multi-agency data sharing, the intention of this document is to replace the need for lengthy future agreements by underpinning them with these guiding principles. It is envisaged that in future all ISAs, current and new, will be short, specific and user friendly.

One of the guiding principles of this agreement is that there is a clear expectation that parties share data in accordance with the requirements of the Data Protection Act 2018, the UK General Data Protection Regulation and any applicable Data Sharing

Code of Practice (Information Commissioners Office (https://ico.org.uk/). There is also an expectation that the terms of the Human Rights Act 1998 and other relevant legislation are adhered to.

This ISA (Tier1) provides an overarching agreement which sets out the guiding principles and ethos of data sharing between the signatories to this. This is signed off once by or on behalf of a chief officer or equivalent for each organisation.

The second tier is the specific agreement between the signatories for the sharing of personal data. An ISA (Tier 2) can be signed off locally by a senior manager or practitioner who has the authority to act on behalf of their organisation. A template that should be used for all future ISA Tier 2's can be found at Appendix A to this agreement.

It is important to note that this is an overarching agreement to formalise the regular sharing of information. It does not interfere with or otherwise prevent the sharing of information on an adhoc basis in accordance with the provision(s) under the UK GDPR and the Data Protection Act 2018.

Data Protection Compliance:

The partners agree that the data sharing under this ISA will involve processing of personal data which must be carried out in accordance with Data Protection legislation (the UK General Data Protection Regulation and/or the Data Protection Act 2018). Personal data should only be shared where it is necessary and lawful to do so. At all times those sharing personal data should remember the need to ensure that such data is processed lawfully and fairly in relation to the data subject. Where personal data is to be disclosed the following sections will apply.

They agree that some of the personal data may be 'special category data' or 'criminal offence data' and some of the processing may be 'sensitive processing' for which sharing can only occur in narrow circumstances.

The partners recognise that dependent on their status and the purpose of the processing that some sharing may be processing for law enforcement purposes while some may be for general purposes.

The partners accept that in terms of Data Protection legislation they are individual controllers in their own right for the personal data held by them under this ISA until the point where that data is shared directly with and received by another partner(s) – at that point the recipient partner(s) will assume individual controllership of their copy of the personal data disclosed to them.

The partners also accept that where data including personal data is 'pooled' together from different partners the pooled data may be subject to joint controllership by each partner that has access to that data. In such circumstances they accept the requirement for a 'Joint Controller Agreement' or equivalent to be in place.

The partners recognise that the purposes for sharing personal data will be specified and made explicit in their privacy policies or data protection policies and their privacy notices (or fair processing notices or data protection notices). They agree to meet any

transparency requirements arising from the Data Protection legislation. It is essential that signatory organisations have also paid the necessary fee to the Information Commissioner as required under the Data Protection Act 2018.

The partners accept that they will never use any personal data shared for a purpose that conflicts with or is not compatible with the purpose(s) for which it was shared unless the law allows that to occur. It is also important that any shared data is held securely and not disclosed onwards without the agreement of the original data controller.

The partners agree to share personal data only where it is lawful and fair to do so, subject to exemptions, and where necessary conditions for the processing have been met.

The partners accept the requirements under Data Protection legislation to maintain respective records of processing activities and agree that this ISA shall be included in such records.

The partners agree to maintain individual records of all data they have shared or received under this ISA and recognise the importance of keeping such records up-to-date.

The partners assert that they have considered their obligations arising from the Data Protection legislation and determined that in principle their sharing of personal data under this ISA is in compliance with Data Protection legislation.

The partners accept that it is their responsibility individually, or jointly in cases where they act as joint controllers, to ensure that on a case-by-case basis sharing of personal data under this ISA and its subsequent use by them is in compliance with Data Protection legislation.

This Agreement and, any Tier 2 Agreements arising from it, will normally be considered as suitable for both internal and external publication.

What data is necessary to exchange?

Each organisation may have its own criteria or restrictions around what data may be provided in certain circumstances, which is a matter for them to consider on each occasion and cannot be prescribed in a document such as this. A Data Protection Impact Assessment should be carried out or a decision not to complete one recorded.

In the case of personal data, the Data Protection Act 2018, the UK GDPR and the Human Rights Act 1998 apply and must be considered at every opportunity. As a general rule there must always be a clear purpose and a relevant legal gateway, and any data provided must be necessary, relevant, proportionate, the minimum necessary to achieve the purpose, and clearly distinguish fact from opinion. This means that even when there is a legal basis to share, it may not be appropriate to share all of the information requested. Every request should be dealt with on a case by case basis.

Retention:

Partners accept that they must only store shared data in a form that identifies individuals for as long as is necessary for the purposes for which they processing the personal data.

The partners also agree that they must each have and implement comprehensive retention schedules which set out the minimum necessary period of storage for different categories of personal data, and are determined taking into account:

- The types of personal data processed (organised, for example, by function);
- The purposes for processing the personal data;
- Why each type of personal data should be retained;
- Any relevant industry standards or guidance;
- Any relevant legal obligations to retain personal data for specific periods of time.
- Set out where the personal data will be stored and how it will be kept secure during the retention periods.
- Set out how any processors who process data on their behalf will comply with their retention periods.
- Set out how data will be archived or destroyed.

The partners agree to have systems in place to adhere to the periods in their Retention Schedules and to review their Retention Schedules regularly. They will train their staff so that they are empowered to comply with their Retention Schedules.

The partners agree that where a partner is disbanded the partner will ensure that the shared personal data held by it is disposed of securely and confidentially. Alternatively, where the partner is replaced by a successor organisation, it will ensure that the personal data held by it is properly transferred to its successor organisation, subject to the successor organisation becoming a signatory to this ISA. If the successor does not wish to become a signatory to this ISA, the personal data will be disposed of securely and confidentially.

Every ISA Tier 2 Agreement will have a retention period recorded which is specific to the information shared.

Information Security:

The partners agree to put in place appropriate physical, technical and organisational measures to protect any data provided to them under this ISA.

The partners accept the requirement to ensure that any personnel are able to access only the shared personal data necessary for their role and that they are appropriately trained so that they understand their responsibilities in relation to personal data and Data Protection legislation.

The partners agree to maintain a high standard of operational security by having and adhering to proper security policies, including physical security policies; IT security policies and business continuity policies.

The partners agree to protect the physical security of the shared data. This means they will, as a minimum:

- Ensure their organisation controls physical access to its premises;
- Ensure visitors to the premises either use only specific areas, or are required to wear visible visitor passes at all times whilst in the premises;
- Ensure proper physical control of printers and photocopiers so that personal data is not left lying on printers/photocopiers;
- Ensure secure disposal of printed materials, so that materials intended for disposal do not remain accessible. This may mean having locked confidential waste bins situated next to printers/photocopiers and in other strategic locations in the premises;
- Ensure that old computers, printers and other electronic equipment are disposed of safely and that all personal data is irretrievably deleted from any memory before disposal.

The partners agree to protect the electronic security of the shared data. This means they will, as a minimum:

- Ensure their organisation has a strong password policy that is adhered to by all personnel. This should include requiring a sufficiently complex password which is never kept with the device. The policy should require the password to be used until users are told to change that password; prevent reuse of passwords over a number of systems and prevent sharing of password among staff members;
- Ensure their organisation installs security patches on electronic devices (including ensuring all operating systems' updates are installed in line with best practice);
- Ensure personnel are given access only to the electronic systems that they need to have. Senior staff may not necessarily need greater access than junior staff. Access rights should be continuously monitored and reassessed when staff members change their work;
- Ensure that any Wi-Fi connections are secure and that any guest Wi-Fi is on a segregated system, so that guests cannot access other systems from that Wi-Fi;
- Ensure that any data that is transferred, either within or outside the United Kingdom, is transferred securely, in line with best practice;
- Ensure that their organisation complies with the best practice of cyber security as detailed by the National Cyber Security Centre.

The partners agree to ensure that all shared data held on portable devices, including laptops, tablets and USB/portable drives, has full disk encryption. This must be to industry standard, and as a minimum:

- FIPS 140-2/256 bit asymmetrical encryption; or
- CBC-AES 256-bit encryption. A recognised mark of excellence in encryption is CCTM government accreditation (for more information, see the National Cyber Security Centre website).

The partners shall e-mail special category personal data or information about individuals' criminal convictions or offences, suspected or otherwise, only via secure e-mail.

The partners agree to have contracts and systems in place to ensure that any contractors and subcontractors managing any aspect of information security are fully aware of and abide by this ISA.

The partners agree to have robust data breach reporting policies in place, and adhere to them, so that all personal data breaches are reported immediately to staff responsible for managing data breaches when such breaches become apparent. Further, partners accept that:

- A "personal data breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which we have transmitted or stored or processed.
- If the personal data breach involved the data shared under this ISA, then the organisation/public body who discovers the breach must immediately inform the other partners involved in the sharing of the personal data, particularly the partner who originally shared the data.
- The partners involved will decide who will take the lead on addressing the breach and on whether the breach needs to be reported to the Information Commissioner or to the individuals concerned without undue delay and usually within 72 hours of having become aware of the breach.
- Personal data breaches should trigger an exceptional review of this ISA.

Data controllers agree to allow relevant signatory organisations, reasonable access to their premises to check[1] the arrangements for the retention, use, disposal and general security of the data shared by them.

Data Quality

The partners acknowledge that they have a general duty to ensure that personal data is accurate, separate to the requirement to take steps where an individual exercises the right to rectification.

The partners therefore agree:

- To have systems in place to identify any personal data that is inaccurate as to any matter of fact.
- That if partner discover that personal data is inaccurate as to any matter of fact, they will ensure that the data is made accurate and will notify any partners with whom they had shared that personal data of the accurate data.
- If they are notified that inaccurate personal data has been shared with them, they will immediately take steps to amend the inaccurate data.
- That opinions are accurate so long as they are correctly recorded. If they discover that an opinion is incorrect (for example because it is based on inaccurate data), then they will record that the opinion is incorrect.

[1] ICO: Data sharing code of practice

- If they discover that they have shared an opinion which is incorrect because it is based on inaccurate personal data, they will notify any partner within whom they had shared the incorrect opinion.
- If they are notified that an incorrect opinion has been shared with them, they will immediately take steps to delete the incorrect opinion, unless it is important to retain a record of that opinion. If so, they will ensure that the record clearly shows the opinion is incorrect.

Complaints and Breaches

The partners agree to have robust data breach reporting policies in place, and adhere to them, so that all personal data breaches are reported immediately to staff responsible for managing data breaches when such breaches become apparent. Further, partners accept that:

- A "personal data breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which we have transmitted or stored or processed.
- If the personal data breach involved the data shared under this ISA, then the organisation/public body who discovers the breach must immediately inform the other partners involved in the sharing of the personal data, particularly the partner who originally shared the data. These should be reported to the Data Protection Officer for each partner organisation, for Avon and Somerset Constabulary these should be reported to DPA Breaches@avonandsomeset.police.uk
- The partners involved will decide who will take the lead on addressing the breach and on whether the breach needs to be reported to the Information Commissioner or to the individuals concerned without undue delay and usually within 72 hours of having become aware of the breach.
- Where there has been a data breach of Data Protection Legislation, the relevant signatory organisation will provide all reasonable, timely and necessary assistance to the respective data controller(s) and the Information Commissioners Office, in order to help manage the breach, prevent further data losses, minimise harm to a data subject and maintain public confidence.
- Personal data breaches should trigger an exceptional review of this ISA.
- If a complaint is received in relation to the sharing of information under this Agreement, the respective signatories will keep each other informed of any developments, progress and lessons learned.

Data subject Rights

The partners recognise individuals whose personal data is shared have a series of rights under the Data Protection legislation and that these will be facilitated.

Each signatory organisation will deal with such requests in accordance with their local arrangements. Where a request involves data originating from another organisation, the receiving organisation shall contact the sharing organisation to advise them accordingly and seek any representations, including whether, for example, an

exemption applies under the Act. However, the decision to disclose rests with the receiving organisation.

Closure/Termination of this Agreement

Each signatory organisation shall at all times maintain the security and integrity of all personal data supplied pursuant to this Agreement. This clause shall survive termination of the Agreement or the withdrawal of or removal of any signatory organisation.

This Agreement will be reviewed every two years. In the event of it being terminated, withdrawn or ceasing to have effect, the Avon and Somerset Constabulary, who host it, will write to all other signatories, giving at least 30 days' notice.

A signatory organisation can withdraw from this Agreement after giving 30 days' notice to the Avon and Somerset Constabulary. In the event of a withdrawal any associated ISA Tier 2's would cease to have effect after the 30 day notice period.

A signatory organisation can be suspended from this Agreement following a major breach of the Data Protection Act or a breakdown in trust, for example. A suspension is likely to be a rare event and will be subject to a Risk Assessment and Resolution meeting. The panel will be made up of the signatories of this agreement, or their nominated representatives. A meeting will take place within 14 days of any suspension. Any associated Tier 2 Agreements will also be suspended accordingly and all reasonable steps must be taken to ensure that no further information is shared under this Agreement or related Tier 2 Agreements during the period of suspension.

It is important to note that the temporary suspension or withdrawal from this Agreement does not preclude the continued adhoc sharing of information with the affected partner if a legal gateway exists. A decision to share information will be made on a case by case basis.

The premature termination of a Tier 2 Agreement before its agreed expiry date should be in writing and will normally take immediate effect.

In the event of a suspension, withdrawal or termination of this Agreement and related Tier 2 Agreements, it is incumbent on the relevant parties to withdraw them from within their respective organisations and public facing sites as soon as practicable, and to communicate the fact to staff, interested parties and the wider public as appropriate.

Nominated Host

The nominated host of this Agreement is the Avon & Somerset Constabulary Data Protection Officer (Compliance), who shall on behalf of the partner agencies:

- Ensure that a review is carried out biennially.
- Facilitate the circulation of all requests for change, co-ordinate responses, obtain agreement for the changes from the signatories to this Agreement and distribute up-dates as these become available.

Signatories:

By signing this document the participant(s) accept the statements, agree to maintain the specified standards, and commit to achieving compliance with any legal obligations.

Signed and dated:

Name:

Position:

Organisation name:

Signed and dated:

Name:

Position:

Organisation name:

Appendix A:

A link to the ISA Tier 2 template can be found here